



Consolidated Space Operations Contract

NASA Integrated Service Network (NISN) Security Management Plan

May 18, 2001

Effective: May 18, 2001

Contract Number: NAS9-98100

Consolidated Space Operations Contract (CSOC)

NASA Integrated Services Network (NISN) Security Management Plan

May 18, 2001

Effective: May 18, 2001

Contract Number: NAS9-98100

Approved by:

 5/15/01

Jim Wairley Date
MSFC Site Security Manager
Consolidated Space Operations Contract

Approved by:

 5/30/01

George E. Grazier, III Date
MSFC Production Operations Manager
Consolidated Space Operations Contract

I have examined the security controls and find that all risks have been reduced to an acceptable level. Risks that remain are not considered significant enough to impede placing the system in normal operation. I, therefore, certify this system for operation for a period not to exceed 36 months or the occurrence of a significant change, whichever occurs first.

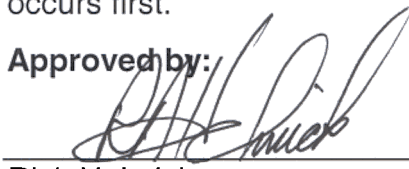
Approved by:


Owen Johnson
NISN Security Manager
MSFC, NASA

5/15/01
Date

I have examined the security controls and find that all risks have been reduced to an acceptable level. Risks that remain are not considered significant enough to impede placing the system in normal operation. I, therefore, certify this system for operation for a period not to exceed 36 months or the occurrence of a significant change, whichever occurs first.

Approved by:


Rick Helmick
NISN Project Manager
MSFC, NASA

5-15-01
Date

Change Information Page

List of Effective Pages			
Page Number		Issue	
Cover		Revision 1	
Signature Page		Revision 1	
Change Information Page		Revision 1	
DCN Control Sheet		Revision 1	
Preface		Revision 1	
vi through viii		Revision 1	
1-1 through 1-10		Revision 1	
2-1 through 2-4		Revision 1	
3-1 through 3-4		Revision 1	
4-1 through 4-6		Revision 1	
5-1 through 5-4		Revision 1	
6-1 through 6-2		Revision 1	
7-1 through 7-14		Revision 1	
A-1 through A-3		Revision 1	
Document History			
Document Number	Status/Issue	Publication Date	Effective Date
CSOC-MSFC-PLAN-001095	Revision 1	May 18, 2001	May 18, 2001

DCN Control Sheet

DCN Number	Date/Time Group (Electronic DCN Only)	Month/Year	Section(s) Affected	Initials

Preface

The purpose of the plan is to provide effective security of National Aeronautics and Space Administration (NASA) Integrated Services Network (NISN) resources.

This document is controlled by Production Operations. This document will be changed by Documentation Change Notice (DCN) or complete revision. Proposed changes to this document must be submitted to Consolidated Space Operations Contract (CSOC) Marshall Space Flight Center (MSFC) Site Security Manager, Jim Worley, along with supportive material justifying the proposed change. Comments or questions concerning this document and proposed changes shall be addressed to:

Jim Worley, CSOC MSFC Site Security Manager
(256) 961-9485
jim.worley@csocoonline.com

Contents

Preface	v
Section 1. Introduction.....	1-1
1.1 Purpose.....	1-1
1.2 Scope	1-1
1.3 Responsibilities	1-2
1.4 References.....	1-2
1.5 Documentation	1-3
1.6 Safety	1-3
1.7 Definitions	1-3
1.8 General Description And Purpose Of NISN	1-5
1.9 System Category.....	1-5
1.10 Overview Of The Security Plan	1-5
1.10.1 NISN System Components	1-5
1.10.2 CSOC-Provided NISN Services	1-6
1.10.3 NISN System Categories	1-10
Section 2. System Identification.....	2-1
2.1 Responsibilities	2-1
2.1.1 NISN Project Office	2-1
2.1.2 NISN Security Manager	2-1
2.1.3 NISN Security Team	2-2
2.1.4 Network Services Group and Support Personnel.....	2-3
2.1.5 Customer Interface Group and Customers	2-3
2.1.6 Business Management Group.....	2-4
Section 3. System Procedure	3-1
3.1 Rules Of The System	3-1
3.2 Use Of Government Resources	3-1
3.3 Conducting Division Business.....	3-1
3.4 NISN Internet Protocol Address Usage.....	3-1
3.4.1 NISN Internet Protocol Address Transfer.....	3-1
3.4.2 NISN Address Block Issuance	3-2
3.5 Personal Use Of Resources.....	3-2

3.6	Misuse Of Resources.....	3-2
3.7	Compliance With Software License Agreements	3-3
3.8	Right To Privacy.....	3-3
3.9	Recording Of Transactions	3-4
3.10	Escorting Personnel Without NISN Access.....	3-4
Section 4. Requirements.....		4-1
4.1	Training Requirements.....	4-1
4.2	Basic Training Requirements	4-1
4.3	Training Offered By Contractors.....	4-2
4.4	Personnel Security Requirements.....	4-2
4.5	External Requirements And Interfaces.....	4-3
4.6	Federal Requirements.....	4-3
4.7	Requests For Personnel Security Investigations.....	4-3
4.7.1	Line Manager Responsibilities	4-3
4.7.2	Means to Initiate an Investigation.....	4-4
4.8	Granting IT Access.....	4-4
4.9	U. S. Citizens And Resident Aliens	4-4
4.10	Foreign Nationals.....	4-5
4.11	International Partners.....	4-5
4.12	Unfavorable Investigation Results.....	4-6
Section 5. Incident Response Capability.....		5-1
5.1	General	5-1
5.2	Mission Statement.....	5-1
5.3	Recognizing An Information Technology Security Incident	5-1
5.4	Reporting An Information Technology Security Incident	5-2
5.4.1	Computer Virus Infections.....	5-2
5.4.2	Other Information Technology Security Incidents.....	5-2
5.5	Handling Evidence Of A Computer Crime.....	5-3
5.6	Handling Incident Information.....	5-3
5.6.1	Quality Records.....	5-3
5.6.2	Forms	5-3
5.7	Returning Equipment To Service	5-4
5.8	Requests For Information By External Agencies.....	5-4
Section 6. Support, Controls and Guidelines.....		6-1
6.1	Continuity of Support.....	6-1
6.2	Technical Controls	6-1
6.3	Security Guidelines	6-1

Section 7. Internet Protocol Operational Network Security Plan7-1

7.1	System Identification	7-1
7.1.1	Responsibilities	7-1
7.1.2	System Name/Title	7-3
7.1.3	System Category	7-4
7.1.4	System Operational Status	7-4
7.1.5	General Description/Purpose of System	7-4
7.1.6	System Environment and Special Considerations	7-4
7.1.7	Point of Contact	7-4
7.2	Sensitivity of Information Handled	7-4
7.2.1	Applicable Laws/Regulations Affecting the System	7-4
7.2.2	General Description of Information Sensitivity	7-5
7.3	System Security Measures	7-5
7.3.1	Risk Assessment and Management	7-5
7.3.2	Applicable Guidance	7-5
7.3.3	Security Control Measures	7-5
7.3.4	Security Control Measure Status	7-6
7.3.5	Security Control Measures for Major Applications	7-8
7.3.6	Contingency Plan	7-12
7.3.7	Audit and Variance Detection	7-12
7.3.8	Hardware/Application Software Maintenance Controls	7-13
7.3.9	Documentation	7-13
7.3.10	Security Awareness and Training Measures	7-13
7.3.11	Technical Controls	7-13

Appendix A. Abbreviations and Acronyms A-1**List of Figures**

Figure 2-1. NISN Security Organization	2-1
----------------------------------------------	-----

List of Tables

Table 7-1. Security Control Measure Status	7-7
--------------------------------------------------	-----

Section 1. Introduction

1.1 Purpose

The purpose of the plan is to provide effective security of National Aeronautics and Space Administration (NASA) Integrated Services Network (NISN) resources.

This document specifies the security roles and responsibilities for the NISN Wide Area Network (WAN) Project. The goal of NISN security is to provide cost-effective protection that ensures the integrity, availability, and confidentiality of NASA data while within the NISN network. This NISN Security Management Plan does not replace any security directives, requirements, or policies created by local NASA centers, NASA Headquarters, or customers, but identifies the roles and responsibilities of the NISN personnel responsible for implementing security and provides the basic requirements for the Security Policy.

The NISN resources to be protected include, but are not limited to, the following: circuits, routers, bridges, hubs, switching equipment, and management monitoring and control devices.

NISN security has the following objectives:

- a. Protect against deliberate or accidental corruption or loss of user data when the data is transported on the NISN WAN.
- b. Protect against deliberate or accidental actions that render the NISN WAN unavailable to users.
- c. Ensure that there is no deliberate or accidental disclosure of sensitive NASA information to unauthorized personnel while within NISN.
- d. Protect against unauthorized access to NISN resources.

1.2 Scope

This NISN Security Management Plan was developed by Consolidated Space Operations Contract (CSOC) in accordance with NASA and Marshall Space Flight Center (MSFC) current directives and practices to safeguard information technology resources and information.

NISN provides WAN communications and networking services to all NASA enterprises, centers, programs, projects, and field locations. NISN communications services include video, voice, facsimile, routed data, and custom services, both domestic and international.

To protect NASA's valuable resources, all Information Technology (IT) systems that use NISN must be designed and operated so that sensitive space communications operations are not interrupted, distorted, or captured by unauthorized parties. An IT system refers to any equipment or interconnected systems or subsystem(s) of

equipment used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and information. This includes mainframe computers, minicomputers, microcomputers, workstations, word processors, automated office support systems, communications systems, networks and their interconnecting hardware, and test equipment.

It's important for NISN/CSOC personnel to follow referenced NASA Procedures and Guidelines (NPG), NASA Standards (STD), NASA Chief Information Officer (CIO) Policy, Office of Management and Budget (OMB) Requirements, Marshall Procedures and Guidelines (MPG), CSOC Central (CEN) Major Processes and Plans, and MSFC Major Processes and Plans that are listed in this plan.

1.3 Responsibilities

The NISN Security Management Plan applies to all NISN individuals across all NASA centers who are serviced by NISN, and to those individuals who participate in the design, development, acquisition, operation, maintenance, management, upgrade, or disposal of IT or telecommunications systems or the information these contain. This NISN Security Management Plan applies only to the security of unclassified automated information, applications, and computer and telecommunications systems for NISN, and it also applies to the elements of confidentiality, integrity, and availability of sensitive information transiting across the NISN infrastructure.

1.4 References

The following documents are referenced in this NISN Security Management Plan:

- a. Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, OMB Circular A-130, Transmittal Memorandum 3, February, 1996.
- b. The Computer Security Act of 1987, Public Law 100-235, January 8, 1988.
- c. Network Protocol, NASA-STD-2806, October 23, 1995.
- d. Security of Information Technology, NPG 2810.1, August, 1999, (Guidance only until contract change).
- e. Security of Information Technology, NPD 2810.1, April 19, 1999.
- f. MSFC Information Technology Security, MPG 2810.1, June, 1998.
- g. Security of Information Technology, MPD 2810.1, November 22, 1999.
- h. CSOC Security Management Plan, CSOC-CEN.SE06.000039, September, 1999.
- i. CSOC Configuration Management Plan, CSOC-CEN.PI03.000032.
- j. Safety and Health Plan, CSOC-CEN.SH20.000041.
- k. CSOC Emergency Preparedness and Disaster Recovery Plan, CSOC-CEN.PO60.000034.

- l. IT Master Plan Process, CSOC-CEN.PM50.001054.
- m. Security Account Administration Process, CSOC-CEN.PM50.001055.
- n. Security Penetration Testing Process, CSOC-CEN.PM50.001061.
- o. Security Engineering and Certification Maintenance Process, CSOC-CEN.PM50.001062.
- p. Security Incident Monitoring and Response Process, CSOC-CEN.PM50.001063.
- q. CSOC Emergency Preparedness and Disaster Recovery Plan (MSFC), CSOC-MSFC-PLAN-000451.
- r. IT Security Alert Notification Process, CSOC-MSFC-MPRC-001237.
- s. Internet Protocol Operational Network (IONet) Disaster Recovery Plan, 290-013, December 2000.
- t. "Limited Personal Use" of Government Office Equipment; NASA CIO acceptable policy: <http://www.cio.gov/files/peruse.pdf>.

1.5 Documentation

The NISN Security Management Plan is augmented by the CSOC Emergency Preparedness and Disaster Recovery Plan (MSFC), CSOC-MSFC-PLAN-000451. Procedures specific to each of the elements covered in the NISN Security Management Plan are addressed in detail in this plan.

1.6 Safety

The NISN program will comply with the requirements of Safety and Health (SH) Plan, Data Requirements Directive (DRD) 2.1.9-a, of the CSOC. Objective evidence of plan implementation, training, and evaluation are available for verification upon request from the SH organization at CSOC Central.

1.7 Definitions

OMB Circular A-130, Transmittal Memorandum 3, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, introduced new terms dealing with IT security that are defined below.

- a. Adequate Security - Security commensurate with the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of information. Adequate security includes ensuring that systems and applications, used by NASA, operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.
- b. Application - The use of information resources to satisfy a specific set of user requirements.

- c. General Support System (GSS) - An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data applications, communications, and personnel. A system can be a Local Area Network (LAN), including smart terminals that support a branch office; an agency-wide communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared Information Processing Service Organization (IPSO).
- d. Major Application - An application that requires special attention to security because of the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of information in the application hereinafter referred to as critical systems.
- e. Privileged Users - The user population who can bypass or modify the technical or operational system security controls.
- f. Ordinary (Non-Privileged) Users - The user population whose ability to read, write, and modify information is specifically limited to that information to which they have been given access.
- g. Limited Users - The user population who may be able to bypass security controls for some portion of the system, but not the entire system.
- h. Push Technology - a server or system that broadcasts outbound traffic.
- i. Special Management Attention - Certain systems and software applications, because of the nature of the information in them or the functions they support, require special management oversight and attention. The CIO, Center IT Security Manager (SM), Organization Computer Security Officials, and line managers are expected to exercise management judgment in determining which of their systems and software applications require "special management attention." Systems designated to be given "special management attention" need to have their security concerns documented and justified in an IT Security Plan. The Organization Computer Security Official and the CIO shall conduct periodic independent reviews and audits of security controls until special management concerns have been alleviated. The following list describes some specific systems that will require special management attention.
 - 1. Major Applications - Use of information and IT to satisfy a specific set of user requirements that require special management attention to security. This attention is required due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.
 - 2. Major Information Systems - Systems that have been designated by the CIO as "major information systems" for OMB A-11 reporting.
 - 3. Mission Critical Systems - Systems that provide agency-wide support, such as WANs, agency-wide business functions, command and control of

space systems, agency-wide consolidated IT resources, or IT resources that affect life support systems.

4. NASA Resource Protection (NRP) Facility - IT resources critical to a facility or operation designated under the NRP program by the cognizant program office (refer to NPD 1600.2, NASA Security Program).
5. Center Designated Systems - Other IT systems designated by the Center Director or CIO.

1.8 General Description And Purpose Of NISN

NISN is the result of the consolidation of the management responsibility for the various NASA WANs under a single organization.

The scope of WAN encompasses a variety of services such as voice, video and data both at the basic transmission level, as well as, the routing of various network protocols. Details pertaining to these systems/services are located in Section 7, Internet Protocol Operational Network Security Plan (IONet). These services satisfy NASA's domestic and international requirements. These network services are provided to all agency customers including mission, programmatic, administrative, and scientific community. Most of the mission requirements for NISN services are received via the Space Operations and Management Office (SOMO) Center Commitments and Mission Services Management, while other requirements are received directly or through center representatives.

1.9 System Category

NISN is categorized as a general support system with special emphasis to security. NISN is a Mission Critical System that provides agency-wide WAN support. As such, the MSFC CIO has designated NISN as a system requiring special management attention and oversight.

1.10 Overview Of The Security Plan

1.10.1 NISN System Components

NISN is grouped by function and services to comprise the following systems:

- a. WAN
- b. Gateways
- c. Enterprise Network Management Center (ENMC)
- d. Premium Internet Protocol (PIP) and Standard Internet Protocol (SIP)
- e. NASA Communications (Nascom)
- f. Mission Video
- g. Dedicated Voice

- h. Video Teleconferencing System (ViTS)/Voice Teleconferencing System (VoTS)
- i. Network Integrated Services Center (NISC)
- j. Facsimile Services

1.10.2 CSOC-Provided NISN Services

The NISN provides for the transport and delivery of NASA WAN communications services. The NISN provides both digital and analog services, dedicated and switched circuits, packet data transport, multi-protocol wide area networking, domain name servers, and various data networks. Voice, video, and facsimile are also available.

Brief descriptions of NISN services follow:

- a. IP Operational Network (IONet) – Based on a Goddard Space Flight Center (GSFC) inter-building Fiber Distribution Data Interface (FDDI) backbone network, with Ethernet, FDDI, and serial WAN extension to users. The IONet supports missions on a 24 – hour basis transferring operational real-time data (attitude, command, orbit, ephemeris, telemetry, state vectors, etc.) as well as non-real-time data (data products, quick-look image data, etc.). Refer to Section 7, Internet Protocol Operational Network Security Plan.
- b. ViTS - The NASA ViTS is a video teleconferencing service providing interactive point-to-point and multi-point conferencing capabilities to NASA locations, selected contractor facilities, and public video conferencing services. The ViTS services include provisioning and maintaining special video conferencing rooms, scheduling of video conferences, and the transmission and distribution of the video and audio among the participating locations.
 - 1. The ViTS is currently based on circuit switching technology and utilizes signal and content compression techniques to enable operation at 112 - 786 kilobytes per second (kbps) standard operation at 384 kbps second.
 - 2. The ViTS rooms consist of multiple cameras, an audio conferencing system, projection screens, and static image graphics capture equipment.
 - 3. Translation among several standard compression formats and speeds is available.
- c. Low Bandwidth Video (LBV) Service - The NASA LBV service is a video teleconferencing system providing interactive point-to-point and multi-point conferencing capabilities to NASA locations, selected contractor facilities, and public video conferencing services. LBV services include provisioning and maintaining portable room systems designed for use by smaller groups, scheduling of teleconferences, and the transmission and distribution of the video and audio among the participating locations.
 - 1. The LBV is currently based on circuit-switching technology and utilizes signal and content compression techniques to enable operation at 112-128 kbps as the standard mode.

2. Translation among several standard compression formats and speeds is available.
- d. Video Distribution Service - The NISN Video Distribution Service provides for the distribution of video signals in support of NASA programs. The particular implementation is dependent on the specific requirements of the program and may involve terrestrial or satellite transmission, with or without the utilization of digital compression and encoding techniques.
 1. This service supports the distribution, on a point-to-point, point-to-multipoint, or satellite broadcast basis, of video signals in support of NASA programs and mandates.
 2. This service supports space flight mission launch activities as well as distribution of NASA programming to the public.
 - e. VoTS - The NASA VoTS provides for the audio meeting and conferencing needs of the Agency. The VoTS provides for the scheduling and setup of operator initiated or meet-me conferences. This service also includes the provisioning and maintaining of room audio conferencing systems. Detailed information on voice teleconferencing options can be found at NISN's website on the Voice Teleconferencing Service Home Page (http://www.nisn.nasa.gov/doc_repos/vots/index.html).
 - f. Dedicated Voice Service - Dedicate Voice Service encompasses a wide range of services and service complexity. At its simplest, it can be a dedicated point-to-point "shout down" circuit with no signaling. However, the majority of Dedicated Voice services consist of a system of highly reliable, dedicated voice circuits working in conjunction with a switching and conferencing system to create voice loops. These voice loops interconnect the various voice distribution systems that support the various mission control centers within the Agency.
 - g. Long Distance Switched Voice Service - NASA's long distance telephone requirements are provided under this service. The service provides both domestic and international long distance dialing services for NASA and selected contractor personnel and includes the provisioning of toll-free inbound (800/888/877 numbers) and calling card services.
 - h. Facsimile Service - Facsimile service includes facsimile machines, secure facsimile machines, and a broadcast facsimile capability. The service includes the centralized procurement and maintenance of facsimile machines in support of all NASA programs. Facsimile broadcast provides the capability for NASA users to send a document to multiple recipients, as established on a preset distribution list, via a single transmission. Secure facsimile machines, designed to interface with cryptographic devices and meet National Security policies, are available by special arrangement.

- i. Standard Routed Data Service - This service provides for basic data networking connectivity through the use of the IP suite. Service and Performance Parameters:
 - 1. Standard IP service is the commodity Internet service that provides the Agency's link to the Internet in general. It provides basic universal Internet connectivity with minimal performance guarantees or restrictions on acceptable use. Standard IP service is open to the public to access publicly available NASA information sources such as World Wide Web (WWW) services.
 - 2. Agency policy (NASA-STD-2806, Network Protocol, October 23, 1995) dictates the use of IP as the agency standard protocol for data networking. Other protocols are supported on a legacy basis only.
- j. Premium Routed Data Service - This service provides a premium level of data networking connectivity through the use of the IP suite. Service and Performance Parameters are as follows:
 - 1. Premium IP service is differentiated from Standard IP service in that it provides a higher performance level, higher priority for problem resolution, and is not directly connected to the general Internet.
 - 2. Premium IP connectivity to the general Internet is through a controlled gateway and is implemented on an exception basis only.
 - 3. Premium IP service is most appropriate for internal agency networking requirements where the agency's operations should be isolated from the general Internet.
 - 4. Agency policy, NASA-STD-2806, dictates the use of IP as the agency standard protocol for data networking. Other protocols are supported on a legacy basis only.
- k. Mission Critical Routed Data Service - This service provides a mission critical level of data networking connectivity through the use of the IP with very controlled access and security measures. Service and Performance Parameters are as follows:
 - 1. Mission Critical IP service is differentiated from Standard IP service in that it is engineered as a very closed system to support space flight mission critical telemetry and data flows. All systems and facilities connected to the Mission Critical IP service must meet the specified Information Technology security level. Access to and from the general Internet and other NASA IP services is extremely limited and on a strict exception basis only.
 - 2. Mission Critical IP service is most appropriate for critical space flight mission support data and telemetry flows that require an extremely high level of availability for mission success and that require no general Internet access.

3. Agency policy, NASA-STD-2806, dictates the use of IP as the agency standard protocol for data networking. Other protocols are supported on a legacy basis only.
- I. Real-Time Critical Routed Data Service - This service provides a mission critical level of data networking connectivity with emphasis on meeting real-time telemetry transport through the use of the IP suite. Service and Performance Parameters are as follows:
 1. Real-Time Critical IP service is primarily differentiated from Mission Critical IP service in that it is engineered with a high level of redundancy to achieve the added level of availability. This service employs the same security and connectivity features and limitations as the Mission Critical service.
 2. Agency policy, NASA-STD-2806, dictates the use of IP as the agency standard protocol for data networking. Other protocols are supported on a legacy basis only.
- m. International Service - International data distribution services are provided to many of NASA's International Partners and agencies through cooperative arrangements. Rather than purchase dedicated circuits for each requirement, cooperative consolidation and integration of various requirements into an economical infrastructure provide the basic connectivity for programmatic requirements for the transport of data, voice, facsimile, electronic mail, and video. To the greatest extent feasible and economical, these gateway and consolidated circuits support all other data distribution services otherwise enumerated.
- n. Custom Services - Custom telecommunication and networking services are specifically designed and engineered to meet unique NASA programmatic requirements. Each program determines the unique attributes of the data distribution services in such terms as security, availability, redundancy, and features that provide the optimum trade-off between cost and program success. Custom Services may be used for both space flight mission critical applications and for general administrative support requirements possessing unique attributes.
- o. Integration and Consulting Service - Whether a customer's requirement is as small as a simple data link between two points, or as complex as a dedicated sub-network for a specific project, consulting and integration services are available to provide the customer with one-stop shopping for the satisfaction of communication and network requirements. If the requirement is unique or does not easily fall within standard service offerings, a consulting staff is offered to work with the customer to provide a tailored solution to the unique needs of a project. Examples of available service include the following:
 1. Requirements Analysis.
 2. Sub-network Engineering and Design.

3. Implementation Coordination.
4. Prototyping Activities.
5. Network Traffic Modeling.

1.10.3 NISN System Categories

These systems are categorized as General Support Systems in accordance with NPG 2810.1. The information categories involved are Mission, Scientific, Engineering, and Research (SER), and Administrative (ADM). Individual security plans for each system are provided as appendixes to this plan. The individual plans address the unique security considerations of each system. The following sections of this document pertain to the overall operation of NISN services and resources.

- a. Section 2, System Identification, describes the NISN security organization and associated responsibilities.
- b. Section 3, System Procedure, describes the responsibilities of all users accessing NISN systems, both privileged and unprivileged. These rules are based on overall results of a risk analysis and apply to the operation of all NISN systems.
- c. Section 4, Requirements, describes the requirements (training, OMB, and NPG/MPG prescribed Security Controls). This section outlines training required for all users that are permitted access to an IT system to the level of the security responsibilities of a designated position. This includes training geared to the privileges of the position that the individual user assumes. In addition, Section 4 details the personnel security controls that the OMB and NPG/MPG prescribe for IT resources.
- d. Section 5, Incident Response Capability, describes how users of the system recognize, respond to, and preserve evidence of any IT security incidents.
- e. Section 6, Support, Controls and Guidelines, describes general procedures in place for the ongoing operations of NISN systems in case of natural or human-caused disasters. Also included is a summary of the technical (logical) controls built into NISN systems. These controls were selected from baseline controls of MSFC Information Technology Security, MPG 2810.1, and from additional controls that risk analysis demonstrated to be necessary to augment baseline controls. User limitations to external access of IT systems are also described in Section 6, along with security guidelines and requirements that apply to NISN systems that interconnect to other NISN systems or outside IT systems.

Section 2. System Identification

2.1 Responsibilities

Security responsibilities will be shared among the NISN Project Office, the NISN SM, NISN Security Team, Network Services Group, Customer Interface Group, Business Management Group, and all Contractor Support Personnel and customers. The security organization for NISN is depicted in Figure 2-1.

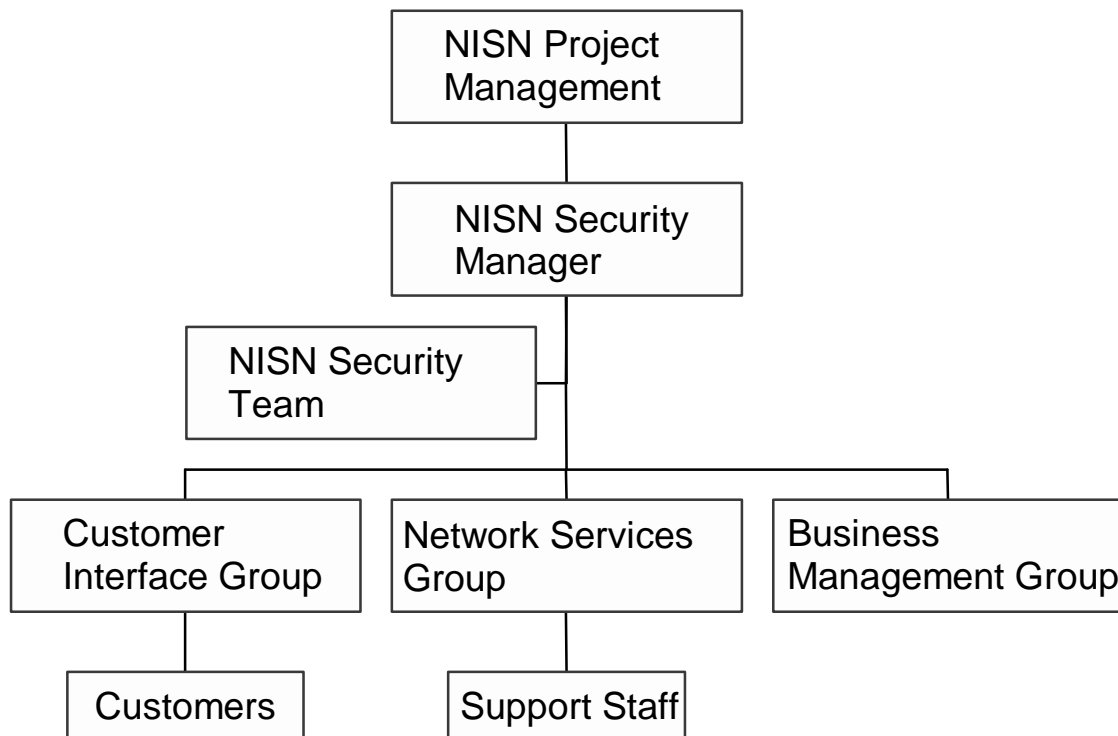


Figure 2-1. NISN Security Organization

2.1.1 NISN Project Office

The NISN Project Office, with the aid of the NISN Security Organization and concurrence of the Production Operations manager, has final authority for security matters. The project office shall maintain close communications with SOMO and with NASA's CIO council.

2.1.2 NISN Security Manager

The SM has the following responsibilities:

- a. Report to the NISN Project Office.

- b. Collect any security incidents within the project and, with the NISN Security Team, determine appropriate action.
- c. Collect waiver requests within the NISN Project Office and, with the NISN Security Team, make recommendations to the project office about the disposition of each waiver.
- d. Ensure that NISN personnel comply with all security policies referenced in this plan and with the agreed-upon sound practices and procedures for protecting the NISN WAN.
- e. Evaluate and ensure that the NISN program has a sound security system that combines education, testing, and technology in the overall security strategy.
- f. Direct the activities of the NISN Security Team with no impact to network operations.
- g. Interface with the Agency Information Technology Security Working Group (ITSWG) to stay informed of the direction the CIOs are taking on security requirements.
- h. Interface with the Principal Center for Information Technology Security (PCITS) to keep abreast of the direction of NASA Information Technology Security standards and recommendations.

2.1.3 NISN Security Team

The NISN Security Team includes the NISN SM, the NASA IT Security Group Program Information Systems Mission Services (PrISMS), and the CSOC/MSFC Security Management Organization.

The NASA IT Security Group is composed of personnel involved in the following five major responsibilities:

- a. Policy and Standardization.
- b. Industrial and Administrative Security.
- c. Telecommunications Security.
- d. Information Technology Security.
- e. Enterprise Security.

The NISN Security Team assists the SM in performing required tasks. The team also has the following responsibilities:

- a. Write and maintain a NISN Security Policy.
- b. Conduct security audits of NISN Sites and equipment facilities and provide written reports to the SM and to other appropriate officials with no impact to network operations.

- c. Review NISN procedures and sound practices to ensure that they comply with the NISN security policy, and to ensure that there are no gaps in the security coverage of NISN resources.
- d. Review the CSOC Configuration Management Plan, CSOC-CEN.PI03.000032, for any needed changes to the configuration of NISN resources.
- e. In accordance with Security of Information Technology, NPG 2810.1, prepare and maintain an adequate risk assessment process -- Security Penetration Testing Process, CSOC-CEN.PM50.001061 -- to appropriately address identified risks; report findings to the SM and other appropriate officials.
- f. Prepare, maintain, and test contingency plans or CSOC Disaster and Recovery Plans, CSOC-MSFC-PLAN-000451.
- g. Generate a waiver when any approved security standard is not being satisfied. Waivers for any known vulnerability that cannot be corrected within 60 days of its identification should be submitted, via the SM, to the NISN project office.
- h. Evaluate system upgrades and new technology to determine if security is adversely affected. Evaluations shall be conducted in a laboratory environment with no impact to network operations.
- i. Review and make recommendations on the disposition of waiver requests.
- j. Maintain consistent and uniform security operations across NISN.
- k. Promulgate policies and directives that describe and enforce the NISN security policy.
- l. Ensure that the interfaces between NISN resources and local users are protected by adequate security measures.
- m. Review security incidents, violations, and written reports sent to the SM when a security incident occurs and recommend corrective actions as necessary.
- n. Ensure adequate security training for NISN Project Office personnel.
- o. Implement security measures to address security vulnerabilities during NISN development.

2.1.4 Network Services Group and Support Personnel

The Network Services Group and support personnel work with the SM and NISN security team on security issues.

2.1.5 Customer Interface Group and Customers

The Customer Interface Group and customers have the following responsibilities:

- a. Work with the Customer and NISN Service Managers to determine, define and document the security requirements for each new service request.
- b. Work with the SM and NISN IT Security Team on security issues.

2.1.6 Business Management Group

The Business Management Group has the following responsibilities:

- a. Provide support in the provisioning and funding of security related products and activities.
- b. Work with the SM and the Security Team on security budget issues.

Section 3. System Procedure

3.1 Rules Of The System

Access to NISN IT resources is a privilege granted to a user in order to perform a required task. The following rules pertain to the overall operation of NISN IT resources along with NASA Acceptable Use Policy (see Universal Resource Locator (URL): [http://www.nisn.nasa.gov/ acceptable.html](http://www.nisn.nasa.gov/acceptable.html)).

3.2 Use Of Government Resources

Federal law, regulations, and agency directives restrict the use of Government computer resources to official business in support of Government contracts and programs. Personal use of Government computer resources is expressly prohibited except for activities sanctioned by NISN management that are open to NISN and/or MSFC and CSOC employees. Violations can result in Federal penalties, up to and including termination of employment.

3.3 Conducting Division Business

The use of Government resources is restricted to conduct the performance of Government business; e.g., the use of Government networks for the transmission of NASA data and Government business development information. The use of Government resources outside the scope of official business requires formal written permission from the NISN Program Manager.

3.4 NISN Internet Protocol Address Usage

All NISN owned IP address must be used on NISN's network for NASA business and in support of NASA projects. These projects may be joint projects with other government agencies, contractors, educational institutions, or non-profit organizations.

3.4.1 NISN Internet Protocol Address Transfer

A NISN IP address can be transferred temporally to an Internet Service Provider (ISP) who is supporting a NASA project under the following conditions:

- a. The NASA project is considered short-term (less that 12 months).
- b. The lead-time on the project makes it impossible for the supporting ISP to obtain the addresses in a timely manner.
- c. The project will have to renumber into new address space that is reserved for this purpose, and cannot be normally assigned IP address space that is a portion of a larger aggregate.

3.4.2 NISN Address Block Issuance

When issuing an “address block” for use by an ISP the following procedure should be followed:

- a. The request needs approval from NISN SM, which will coordinate with NISN Project Management.
- b. The request for the address block must be routed between CSOC WAN engineering and PrISMS Network Information Service (NIS).
- c. All NASA IT SMs will be informed of the fact that the NASA NISN address block is being used and routed by a non-NASA ISP, giving the various IT SMs the opportunity to modify their security policy, if necessary.

3.5 Personal Use Of Resources

Personal use means activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. All employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization. Complete details of authorized and unauthorized use is located in the following document, “Limited Personal Use” of Government Office Equipment per NASA CIO acceptable use policy - <http://www.cio.gov/files/peruse.pdf>.

3.6 Misuse Of Resources

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of government office equipment includes:

- a. Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, greeting cards, video, sound or other large file attachments can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
- b. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.
- c. Using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to inappropriate language, or material that ridicules others on the

basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

- d. The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.
- e. The creation, downloading, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc.
- f. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).
- g. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- h. Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained or uses at odds with the agencies mission or positions.
- i. Any use that could generate more than minimal additional expense to the government.
- j. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

3.7 Compliance With Software License Agreements

All NISN users are responsible for complying with vendor requirements of software copyrights and licenses related to vendor software packages and associated material.

3.8 Right To Privacy

Information on Government IT systems is not to be considered personal or private. No expectations of privacy exist when using Government systems. These systems are not to be used to send, receive, or store any information that users want to keep private. Computer resources, including all forms of electronic storage media, are subject to management inspection or monitoring at any time, and are subject to possible Government inspection or monitoring in accordance with applicable laws, regulations, or agency directives. Findings obtained in this manner can be used in the determination of appropriate disciplinary actions for infractions. Under certain circumstances, the Government can be required to provide computer information to outside parties, such as law enforcement officials.

By using or simply accessing (logging on to) Government computers processing Government information, users are deemed to have given consent for activities to be monitored to the extent permitted by U.S. law, NASA, and MSFC directives. NISN managers are obliged to protect Government property and protect the information entrusted in accordance with contracts or other agreements. This protection is provided through passwords, audit trails, and other computer security measures, to enforce access restrictions described in this plan. System managers monitor computers to detect unauthorized activity, which can include network traffic analysis and keystroke monitoring under circumstances permitted by U.S. law and NASA directives.

If inappropriate activity is detected, the user's account responsible for that activity is subject to immediate termination. Furthermore, the user's system manager is obliged to report inappropriate activity to the appropriate Information Systems Security Official (ISSO) who, in conjunction with the Organization Computer Security Manager (OCSM), involves the Office of Inspector General (OIG) and law enforcement officials for further investigation or prosecution.

Should the inappropriate activity be detected by a NASA IT Security Team at a Site, the NISN SM is responsible to report the inappropriate activity to the affected Center's IT SM only. Further involvement at other centers shall be left solely at the Center IT SMs discretion.

3.9 Recording Of Transactions

Records of computer transactions are maintained in several ways: workstation software can automatically save a copy of whatever a person is working on, whether requested by the user or not; servers may keep records of workstation activities. Copies of these records are routinely made in the event of server crashes and can be maintained for years. Internet sites routinely keep records of who logs in and activities of users.

3.10 Escorting Personnel Without NISN Access

Unauthorized personnel are not permitted in the facility. No unauthorized person is permitted in the controlled access areas of NISN facility. All visitors requiring access must be signed in and out, and be issued a temporary badge by Center Security. Authorized personnel must escort visitor and temporary employees while visiting the controlled access areas of NISN facilities.

Section 4. Requirements

4.1 Training Requirements

All NISN employees receive IT security training commensurate with duties performed. The requisite training is accomplished before the employee performs IT-related duties (before the employee is issued a user account).

4.2 Basic Training Requirements

The supervisor or authority that grants a user ID on a NISN IT system ensures that the user understands at a minimum the following:

- a. IT resources are provided for official business only. User accounts are the property of the Government, not the individual. Complete details of authorized and unauthorized use is located in the following document, "Limited Personal Use" of Government Office Equipment per NASA CIO acceptable use policy - <http://www.cio.gov/files/peruse.pdf>.
- b. Users must abide by all software licensing agreements pertaining to the authorized software they install. To determine if a software package is authorized for installation, check with the MSFC Maintenance Manager.
- c. Software brought into the NISN community must be determined to be free of malicious code before it is used. Users can contact the OCSM or system administrator for assistance.
- d. Users' activities are subject to audit by computer security officials at any time. By logging onto a Government computer, a user is deemed to have given consent to have all activities monitored, including keystroke monitoring.
- e. Users can be liable for activity that takes place on individual accounts. Confidentiality of passwords or other such devices as smart cards that authenticate the authorized user should be carefully maintained. Passwords are changed regularly in accordance with the requirements of NPG 2810.1.
- f. Terminals and workstations are not left unsecured while logged onto a host computer, server, or network.
- g. Users of Government computers have no expectation of privacy. Under the proper circumstances, any information in a user's account can be made available to supervisors; managers; CIO; CCSM; or personnel of the Legal Office, Human Resources Offices, or law enforcement.
- h. Users should use common sense and good judgment at all times. The Internet is an extremely useful tool in accomplishing many tasks. Users should remember that an electronic fingerprint in the form of a NASA ID is left everywhere the user goes on the Internet.

- i. Users may make infrequent personal use of electronic mail (e-mail). Analogous to use of a Government telephone, a user may occasionally contact physicians, dentists, spouses, dependents, or persons handling vehicle repairs or child care when communications cannot reasonably be made during non-business hours or when an urgent need exists.
- j. Misuse of NISN resources can be grounds for withdrawal of IT privileges or disciplinary action. If the misuse violates Federal or state law, civil or criminal prosecution can result. Users should be aware that using a Government computer to store, display, or transmit sexually explicit images, messages, or cartoons or to send messages that contain ethnic slurs, racial epithets, or anything that could be construed as a threat, harassment, or disparagement of others is specifically prohibited. Chain letters are prohibited. Attempting to exceed the privileges granted by a user's account is prohibited.
- k. Each IT security incident or suspected incident is to be reported in accordance with Section 5.4, Reporting an Information Technology Security Incident.

The provisions above represent the minimum mandatory training for all NISN users. No written acknowledgment is required. By logging on to a NISN supported system, a user has acknowledged understanding of these basic rules. A user with questions regarding the appropriate use of NISN resources may ask a supervisor, OCSM, the CIO, the CCSM, or the Legal Office or Human Relations Office personnel for assistance.

4.3 Training Offered By Contractors

Each NISN contractor provides appropriate IT security training for each employee who has access to NISN resources under that contractor's account. An initial orientation briefing that covers at a minimum the basic training requirements described above is sufficient to permit the employee to be granted an unprivileged user account. Contractors provide annual refresher training for employees who are to access NISN resources.

Because organizational needs differ, organizations are responsible for providing IT security training in areas that are peculiar to their needs. If organization level training is needed, the concerned OCSM ensures that appropriate personnel receive training, including civil servants, contractors, international partners, collaborative researchers, grantees, and individuals who use the organization IT systems. Both initial training and periodic retraining are required. The CSOC MSFC Site Security group will track, schedule, and maintain records for all employees.

4.4 Personnel Security Requirements

This section provides the policy and information needed to adequately control privileged user accounts and limited user accounts in accordance with Management of Federal Information Resources/Security of Federal Automated Information, OMB Circular A-130 (revised), and Security of Information Technology, NPG 2810.1. The process to obtain security investigations, which is a requirement for privileged and limited users, is also discussed.

Managers grant access as risk decisions, weighing the potential costs and benefits to the Government. Except where specifically limited by Federal directives, managers are free to grant access as desired, upon understanding and accepting the risks.

Privileged and limited users have the authorization to alter or circumvent an operating system or system security protections. Monitoring privileged users is vital to ensure that privileges are not abused. A privileged program is an executable file that has the capability to override or bypass system security measures or system privileges when executed.

On most multi-users' computer systems, privileged users' accounts exist that have complete access to the systems. A user accessing the system with one of these accounts can run any program, change any data, and access any device. For this reason, privileged user accounts should be the most highly protected accounts.

- a. Privileged programs are protected via the permission set in the operating system.
- b. Security administrators can alter the default permission scheme of the directory structure and data files ensuring a predetermined set of access conditions are met.

4.5 External Requirements And Interfaces

There are no external requirements or Interfaces related to the activities in this plan.

4.6 Federal Requirements

Federal directives impose only one limit on line managers to grant access to their systems: users who can bypass technical or operational system security controls are to complete a personnel security investigation with favorable results before access is granted. Managers cannot accept the risk of granting access while the investigation is in progress. The level of investigation to which this category of user is subjected depends on the risk or magnitude of harm that the user can cause. The investigation is renewed at periodic intervals.

4.7 Requests For Personnel Security Investigations

The Security Branch at each NASA Center is the only organization authorized to initiate or conduct personnel security investigations. Line managers do not conduct, contract for, or otherwise participate in personnel security investigations.

4.7.1 Line Manager Responsibilities

- a. Identifying individuals who require privileged or limited access.
- b. Providing the full name, level of privileges required, and contact information for the individual to the Center Security Branch, Personnel Security Group.

4.7.2 Means to Initiate an Investigation

Line managers submit names to the Security Branch using one of the means described below:

- a. For civil servants, the OCSM or administrative officer is assigned the responsibility for collecting and submitting names and privilege levels required.
- b. For contractor personnel, each contractor has a Facility Security Officer (FSO) who submits names and privilege levels required.
- c. Investigations of international partners who seek privileged access to U.S. Government IT systems pursuant to an international agreement are investigated by NASA Headquarters only.

Upon receipt of the information, the Security Branch initiates the investigation by contacting the individual with a request for information and the investigation proceeds. The Security Branch reports a favorable or unfavorable result back to the requesting line manager in accordance with Security Branch directives.

4.8 Granting IT Access

Managers may encounter three groups of users desiring access:

- a. U.S. citizens and resident aliens.
- b. Foreign nationals who are not international partners and are hired by contractors in the normal course of business.
- c. Foreign nationals who are international partners and seek access to NISN IT resources under the terms of an international agreement.

Granting access is a risk avoidance/acceptance process. To grant access to systems and or resources, line managers must be satisfied with the answers to the questions below for each type of user.

4.9 U. S. Citizens And Resident Aliens

The following questions provide assistance to line managers granting access to U.S. citizens and resident aliens:

- a. Is there a valid requirement for a user to have access to a computer?
- b. Has an appropriate personnel security investigation been successfully accomplished for the user who requires privileged or limited access?
- c. Does the user understand the limits of access being granted?
- d. Has the user received the minimum training required?
- e. Is there information on the computers to which the user has access that is inappropriate for the user to possess? If so, adequate controls must be in place to prevent unlawful or improper access or access should be denied.

- f. Does the computer track and log security-relevant transactions sufficient to monitor user access limitations?
- g. Does the Line Manager acknowledge responsibility for granting access with knowledge that granting access to this individual is in the best interests of NASA?

4.10 Foreign Nationals

The following questions provide assistance to line managers granting access to foreign nationals who are not international partners:

- a. Is there a valid requirement for this foreign national to have access to the computer?
- b. Is access requested for a non-privileged account only? (Privileged and limited access is not authorized for foreign nationals who are not international partners.)
- c. Does the foreign national understand the limits of access being granted?
- d. Has the foreign national received the minimum training required?
- e. Is there technological information on the computers that is embargoed from foreign export under U.S. law? If so, adequate controls must be in place to prevent unlawful or improper access or access should be denied.
- f. Is there other information on the computers to which the foreign national will have access that is inappropriate for the foreign national to possess? If so, adequate controls must be in place to prevent unlawful or improper access or access should be denied.
- g. Does the computer track and log security-relevant transactions sufficient to monitor foreign national access limitations?
- h. Does the line manager acknowledge responsibility for granting access with knowledge that granting access to this individual is in the best interests of NASA?

4.11 International Partners

The following questions provide assistance to line managers granting access to international partners:

- a. Is there a valid requirement for these international partners to have access to the computer?
- b. Is an appropriate personnel security investigation complete for the international partners who require privileged access or access with limited system privileges? (NASA Headquarters handles investigations for international partners. Names and privilege levels required are submitted through the Security Branch.)

- c. Does the international partner understand the limits of access being granted?
- d. Has the international partner received the minimum training?
- e. Is there technological information on the computers to which the international partner will have access that is embargoed from foreign export under U.S. law or is not approved for export under the international partner's international agreement? If so, appropriate security controls must be in place or access must be denied.
- f. Is there other information in these computers to which the international partner will have access that is inappropriate for the international partner to possess? If so, adequate controls must be in place to prevent unlawful or improper access or access should be denied.
- g. Does the computer track and log security-relevant transactions sufficient to monitor international partner access limitations?
- h. Does the line manager acknowledge responsibility for granting access with knowledge that granting access to this individual is in the best interests of NASA?

4.12 Unfavorable Investigation Results

Individuals can be denied privileged IT access as a result of a personnel security investigation. The individual has the right to appeal. Personnel should contact their Center Security Branch for more information.

Section 5. Incident Response Capability

5.1 General

A security incident is any event, suspected event, or discovery of a vulnerability that could pose a threat to the confidentiality, integrity, or availability of supporting systems, applications, or information. Each user has the obligation to report observed or suspected security incidents. Any event that a user feels is suspect should be reported immediately to a systems administrator, the computer security official, the systems manager, and the ISSO.

5.2 Mission Statement

The mission of the Intrusion Detection Systems is to send an alert or alarm whenever attempted are made against NASA centers to disrupt or interrupt service, as well as gather evidence needed for criminal proceedings in cases where legal action is warranted. These alerts and alarms result in further investigation and when warranted, corrective action, to prevent abuse and misuse.

5.3 Recognizing An Information Technology Security Incident

Users should watch for the following security incidents:

- a. Files that should be accessible to a user are suddenly unavailable.
- b. A user's account suddenly becomes active, but the user is absent and known not to be using it remotely.
- c. System logs record numerous unsuccessful log-on attempts, but the user is not the one who attempted these log-ons.
- d. Files are edited when no changes should have occurred.
- e. Application software was modified, but changes are not approved by either management or an appropriate configuration control board.
- f. Sensitive material normally handled carefully is found in printer trays or left uncontrolled in work areas.
- g. Unauthorized personnel are discovered in the work area.
- h. Files appear, disappear, or undergo significant and unexpected changes in size.
- i. User accounts appear or disappear from the system without the knowledge or consent of the system administrator.
- j. Parts or all of the system logs are missing, or logs appear altered.
- k. A user's password is changed without the user's knowledge or involvement.

5.4 Reporting An Information Technology Security Incident

Personnel who use NASA IT systems and resources is obliged to report incidents or suspected incidents per Security Incident Monitoring and Response Process, CSOC-CEN.PM50.001063, and relevant guidelines, or others as contractually identified.

In any actual or suspected IT security incident, the following priorities apply:

- a. Protect Government IT resources and information and assist the affected facility to return to normal operations.
- b. Collect information to support criminal, disciplinary, or other appropriate actions against perpetrators.

5.4.1 Computer Virus Infections

Each computer virus infection is a reportable IT security incident. Because viruses are the most common IT security incident in the NASA community, all user workstations should have current antiviral software installed. When the antiviral software alerts users to the presence of a virus, users can employ an available self-repair function provided by the software or they can call the Help Desk. Users who successfully remove the virus using the self-repair function should report the following information to their OCSM:

- a. User's name, mail code, telephone number, and company affiliation.
- b. Location of the workstation.
- c. Name of the virus and date removed.

No further user action is necessary. If the antiviral software also incorporates an auto-reporting capability as part of the software, no report from the user is required because the report is automatically generated and transmitted. Onsite users unfamiliar with the automatic repair of viruses or uncertain of what actions to take should call the Help Desk. If the virus begins to execute and the user believes that the virus is damaging files on the workstation, the user should immediately shut down the workstation by turning off the power and calling the Help Desk.

5.4.2 Other Information Technology Security Incidents

Members of the NISN community who discover an IT security incident should proceed as follows:

- a. Immediately notify the System Security Administrator, supervisor, and OCSM. Leave the equipment alone. Do not try to process, insert, or delete information on the affected equipment.
- b. Immediately notify the CCSM, NISN Security Team, or the Deputy CCSM, and await assistance.

5.5 Handling Evidence Of A Computer Crime

The Intrusion Detection System consists of two parts: (1) network monitoring systems, packet capture and pattern matching, co-located at the NASA centers; and (2) a main monitoring system located at MSFC. The capture packet systems record network traffic for subsequent intrusion analysis. It also has filters to detect abnormal patterns associated with attempts to compromise or deny service. It is further augmented by a pattern matching system that looks for signatures of attempts to compromise an information system or systems that have been compromised. Together with the remote systems, it generates alerts and alarms of intrusions and has utilities to support detailed analysis of intrusion attempts. This data can be saved for evidence or analysis of new attacks.

5.6 Handling Incident Information

Information regarding an IT security incident is sensitive and is disclosed on a strict need-to-know basis only. Without analysis, computer crimes, maintenance problems, and operator errors often look alike. When an incident is discovered, the affected System Management obligation is to preserve the available evidence. An investigator will interview individuals and ask for the following applicable items:

- a. Audit trails or system logs.
- b. Reports of security-relevant events extracted from more extensive system logs.
- c. System monitoring reports.
- d. Documentation to help understand the affected system or its connectivity.

Individuals who have knowledge of the incident should exercise caution to keep information within prescribed channels.

5.6.1 Quality Records

The following items are considered as Quality Records and are controlled in accordance with CSOC Standard Operating Procedure (SOP) for Control of Quality Records, CSOC-CEN-SOP-000216.

- a. Risk Assessment Document located at the Center IT SM Office.
- b. Security Audit Results.
- c. Security Training Records for all CSOC MSFC employees.
- d. System Upgrades Evaluations in agreement with NASA Principal Center of Communications Architecture (PCCA).

5.6.2 Forms

No forms are generated by this plan.

5.7 Returning Equipment To Service

The NISN SM and the IT Intrusion Detection and Incident Response Team's endeavor to return equipment to service as quickly as possible following an incident. In most cases, equipment is returned to service the same day. When a complete backup of the computer or computers involved in an incident is made, the equipment can be returned to service (after a post-risk assessment is made for NISN resources and non-NISN systems, the acceptable use policy applies [see URL: <http://www.nisn.nasa.gov/acceptable.html>]). If the seriousness of an event warrants, equipment may be removed from the area to be held as evidence.

5.8 Requests For Information By External Agencies

NISN furnishes such information as logs of system use to appropriate Federal, state, or local law enforcement officials investigating computer crime. Requests for information from external law enforcement agencies in support of criminal investigations are made to the NISN SM through the Center IT SM.

Section 6. Support, Controls and Guidelines

6.1 Continuity of Support

Continuity of support plans are unique to each component of NISN; the plans are discussed as components of the security plans of the systems presented in the appendixes in a separate document; CSOC Emergency Preparedness and Disaster Recovery Plan (MSFC); CSOC-MSFC-PLAN 000451; July 1, 1999.

6.2 Technical Controls

The technical controls for each system/service will be addressed within each individual system/service plan within NISN.

6.3 Security Guidelines

Security Guidelines will be addressed in the form of Standard Work Instructions, Standard Operating Procedures, Project Plans and Other NASA Documentations/Regulations pertaining to the NISN contract. Awareness programs and in-house training will also be used to ensure employee awareness of security policies/procedures and guidelines.

Section 7. Internet Protocol Operational Network Security Plan

7.1 System Identification

7.1.1 Responsibilities

7.1.1.1 General

The organization responsible for monitoring and ensuring the compliance of the IONet with NASA security policies is the Information Services and Advanced Technology (ISAT) Division Code 290, NASA, GSFC, Greenbelt, Maryland. The following paragraphs detail the responsibilities of key personnel in implementing this IONet Security Plan.

a. ISAT Division Chief

The ISAT Chief has overall responsibility for the security of all systems within the ISAT, including the IONet. In regard to the IONet, the Chief:

1. Makes sure that the security of the IONet is within the bounds of established government and agency requirements.
2. Establishes overall IONet security policy and guidelines.
3. Appoints the ISAT Network Security Officer (NSO).

b. Services and Advanced Technology (SAT) Configuration Control Board (CCB) chairperson

1. Establishes and maintains the IONet configuration management program.
2. Approves all IONet security plans and any subsequent changes.

c. IONet NSO

1. Prepares and implements IONet risk analysis, risk management, disaster recovery, and security plans, and all subsequent changes.
2. Establishes effective security training and awareness programs.
3. Coordinates security policy and activities with the Network Engineering Team Lead.
4. Conducts periodic security audits through a Security, Test, and Evaluation (ST&E) program.
5. Reports IONet security incidents as required by law.
6. Plans and budgets for security related items in order to carry out procedures and controls.

7. Establishes, maintains, and participates in the IONet configuration management program, and the GSFC continuing compliance program.
 8. Establishes and maintains procedures for the effective implementation of physical, personnel, and information technology security within the IONet.
 9. Specifies the system sensitivity and identifies all sensitive files on the IONet.
 10. Directs the support contractor(s) in security operations at the IONet facilities.
 11. Report security incidents in accordance with Security of Information Technology, NPG 2810.1.
- d. Network Engineering Team Lead
1. Implements developed IONet security procedures and controls.
 2. Coordinates security activities with the NSO.
 3. Appoints the IONet Network Manager and IONet System Engineer(s).
- e. IONet Network Manager (NM)
1. Implements software and hardware within configuration management boundaries.
 2. Coordinates with and assists the NSO in the preparation of security plans.
 3. Coordinates and works with the NSO to prepare and implement security procedures and controls.
 4. Reports all security incidents to the NSO.
- f. IONet System Engineer
1. Assists in the preparation and implementation of software and hardware within configuration management boundaries.
 2. Works with the NM to implement security procedures and controls.
 3. Reports all security incidents to the NSO.
- g. NASA Center and Organizational Computer Security Officials with Interfaces to IONet
1. Adhere to all local security requirements and, Security of Information Technology, NPG 2810.1.
 2. Follow the rules of IONet Access Protection Policy and Requirements, 290-004.
 3. Provide a secure environment for the IONet equipment and computers connected to the Closed Segment.
 4. Run logging software if connected to a local network.

5. Ensure equipment is not connected to both the Open and Closed Segments.
 6. Report all security incidents to the NSO.
 7. Submit a completed security checklist with connection request or when requested by Code 290 (usually once every three years) or when major changes to connectivity occurs (see IONet Access Protection Policy and Requirements, 290-004, for checklist)
 8. Provide Computer Security Awareness Training.
 9. Provide data integrity.
- h. International Partners and Contractors
- Follow the IONet Access Protection Policy and Requirements, 290-004.
- i. System Users
1. Submit a formal request for a User ID.
 2. Follow all developed security procedures.
 3. Follow IONet Access Protection Policy and Requirements document 290-004.
 4. Report all security incidents to the NSO.
 5. Attend Computer Security Awareness Training.
 6. Take responsibility for protecting the data.
 7. Sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which they are granted access.
- j. ISAT Audit Team
1. Review all checklists submitted with circuit requests and make recommendations to NSO.
 2. Perform periodic audits of all facilities.
 3. Run scan programs as requested by the NSO.
 4. Evaluate new technology as agreed to by the NSO.
 5. Work with projects and users to ensure protection of the IONet resources.
 6. Evaluate and make recommendations to the NSO on waiver requests.

7.1.2 System Name/Title

IONet includes both Open and Closed Segments with the Internet Protocol (IP) Transition network an integral part of the Closed Segment.

7.1.3 System Category

The IONet environment is considered a major application in accordance with Security of Information Technology, NPG 2810.1.

7.1.4 System Operational Status

The IONet network is fully operational.

7.1.5 General Description/Purpose of System

The IONet is based on a GSFC inter-building FDDI backbone network, with Ethernet, FDDI, and serial Wide Area Network (WAN) extensions to users. These users are U.S. government, international partners, and contractor facilities and employees located both inside and outside the United States.

The IONet supports missions on a 24-hour basis transferring operational real-time data (attitude, command, orbit, ephemeris, telemetry, state vectors, etc.) as well as non-real-time data (data products, quick-look image data, etc.). The network is divided into two parts: the more secure Closed Segment and the less secure Open Segment. ISAT maintains a Secure Gateway (firewall) to prevent penetration of hosts on the Closed Segment from less secure networks. Hosts on both the Open and Closed Segments must provide their own security. At a minimum, all hosts must adhere to the security requirements listed in this plan.

7.1.6 System Environment and Special Considerations

The heart of the IONet (network management system, major network switches, hubs, and routers) is located at GSFC. However, other NASA Centers, universities, contractor locations, and international partners connected to the WAN have equipment to connect these locations to the IONet (such as routers, switches, and hubs). This equipment is configured and controlled by the Network Operations Control Center at GSFC. However, these external locations have local LANs and connections to other networks that are not directly controlled by IONet personnel.

7.1.7 Point of Contact

IONet Network Security Officer
Code 291
Goddard Space Flight Center
Greenbelt, Maryland 20771

7.2 Sensitivity of Information Handled

7.2.1 Applicable Laws/Regulations Affecting the System

The following documents are applicable:

- a. Security of Information Technology, NPG 2810.1.

- b. IONet Access Protection Policy and Requirements, 290-004.
- c. ISAT Configuration Management Plan, 290-001.
- d. Security Procedures and Guidelines, NPG 1620.1.

7.2.2 General Description of Information Sensitivity

System sensitivity and criticality was determined in accordance with the requirements delineated in Chapter 4, Section 4.2.9 of Security of Information Technology, NPG 2810.1. Both the Open and Closed Segments have been determined to be in the Mission (MSN) category. This means if the information, software applications, or computer systems are altered, destroyed or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency Mission. The Closed Segment handles the data that is critical for Mission Operations while the Open Segment handles mission, real-time, and non-real time mission and scientific instrument data.

Security of Information Technology, NPG 2810.1, clearly directs system and process owners to take full responsibility for their security concerns and data. These guidelines also enumerate specific guidelines for WAN and other network services for the purpose of securing the networks, not the data they transport.

7.3 System Security Measures

7.3.1 Risk Assessment and Management

Risks to the Closed IONet and Open IONet due to unauthorized access of resources, modification of data, or denial of system availability are considered HIGH.

7.3.2 Applicable Guidance

Security of Information Technology, NPG 2810.1, was utilized in the development of this security plan.

7.3.3 Security Control Measures

Physical access to the IONet resources is restricted with door locks and limited access requirements. IONet resources must only be used for NASA mission purposes (i.e. no administrative traffic permitted). System access is controlled by passwords with a minimum length of eight alphanumeric and special characters in length (see section 3.11.1 for details). File permissions are implemented within the system to control user access to and use of files. Daily and weekly backups are made of critical software and configuration files.

Projects/users on either the Open or Closed Segments must provide security for their workstations and applications, and are subject to an audit by the ISAT audit team to ensure provision of adequate security for network resources, and to prevent propagation of an infiltration.

7.3.4 Security Control Measure Status

A quick reference to the current status of the security control measures of the IONet can be found in Table 7-1, Security Control Measure Status. It is recommended that each center, contractor location, and International partner complete a similar table. Remarks contained in the status portion of the table are defined as follows:

- a. In Place - Control measures of the type listed are in place and operational, and judged to be effective.
- b. Planned - Specific control measures (new, enhanced, etc.) are planned for the system. A general description of the planned measures, resources involved and expected operational dates are provided if essential.
- c. Not Applicable - This type of control is not needed, cost-effective, or appropriate for the system covered by the plan.

Table 7-1. Security Control Measure Status

Security Controls	In-Place	Planned	Both I & P	Not Applicable
<i>a. Management Controls</i>				
1. Assignment of Security Responsibility	X			
2. Risk Analysis	X			
3. Personnel Screening	X			
<i>b. Development and Implementation Controls</i>				
1. Acquisition/Security Specifications	X			
2. Design Review and Testing	X			
3. Accreditation/Certification	X			
<i>c. Operational Controls</i>				
1. Physical/Environmental Protection	X			
2. Production, I/O Controls	X			
3. Emergency, Backup, Contingency Plan	X			
4. Audit/Variance Detection	X			
5. Hardware/System, Software Maintenance Controls	X			
6. Documentation	X			
<i>d. Security Awareness</i>				
1. Training	X			
<i>e. Technical Controls</i>				
1. User ID & Authentication	X			
2. Authorization/Access Controls	X			
3. Data Integrity/Validation	X			
4. Audit Trails/Journaling	X			
<i>f. Security Controls</i>				
1. Applications	X			

7.3.5 Security Control Measures for Major Applications

7.3.5.1 Management Controls

The IONet has been identified as an IT resource that requires “Special Management Attention” as outlined in Security of Information Technology, NPG 2810.1. Therefore, systems connected to this IT resource need to have their security concerns and their justification documented in an IT Security Plan. The IONet has also been characterized as a NASA Resource Protection (NRP) facility. This requires a background investigation of all persons that are granted unescorted access to designated IONet facilities or areas. See Security of Information Technology, NPG 1620.1, for a full description of the NRP program.

7.3.5.1.1 Assignment of Security Responsibility

Appendix A provides a list of the security responsibilities of the various personnel in implementing this IONet Security Plan.

7.3.5.1.2 Personnel Screening

Some positions require special access privileges in order to perform their assigned duties. Since personnel in these positions can affect the integrity, efficiency, or effectiveness of the network, they require screening for suitability, prior to being granted access.

For GSFC (NASA and contractor) employees, this screening processing is coordinated by the GSFC Security Office and performed by an appropriate Government Agency. For non-GSFC (NASA and contractor) employees, a current Federal investigation performed by the user's parent organization is acceptable. International partners seeking access to U.S. Government IONet resources pursuant to an international agreement must be investigated. NASA Headquarters handles all investigations for representatives of foreign governments (see Security of Information Technology, NPG 2810.1, section 4.5.5.b). In addition, everyone with access to the IONet equipment must have a need-to-know.

Need-to-know is a determination that a prospective recipient of the information, or access, requires the information or access in order to perform tasks or services essential to fulfilling his/her job. Determination of the need-to-know is based upon job assignment and requires the approval of the IONet Network Security Officer (NSO) or his representative.

All personnel having access to the Closed IONet network control devices must undergo a minimum of a National Agency Check.

7.3.5.2 Certification

The IONet has received authorization to process by the GSFC Designated Approving Authority (DAA). The authorization to process is renewed every two years.

7.3.5.3 Operational Controls

7.3.5.3.1 Software Restrictions on Closed Segment

The following software restrictions apply to systems on the Closed IONet:

- a. Penetration testing, such as network scanning, by the project is prohibited. Projects can request the NSO to perform penetration testing. All penetration tests will be conducted by ISAT Personnel.
- b. Network scanning of a project's local sub-network by the project is permitted if prior NSO authorization is obtained.
- c. Projects may have Intrusion Detection Systems (IDSs) on their own sub-network. Prior NSO authorization must be obtained. All components of the IDS must be within the project's local Closed IONet sub-networks.
- d. Transmission of outbound X-Terminal displays is prohibited.
- e. Inbound FTP sessions must be limited and approved by NSO.
- f. Inbound telnet sessions are prohibited.
- g. Software development is prohibited on equipment connected to the network.
- h. Virtual Private Networks (VPN), or encrypted tunnels, within the closed IONet must be authorized by the NSO on a case-by-case basis.
- i. Project firewalls are prohibited.

7.3.5.3.2 Software Restrictions on Open Segment

The following software restrictions apply to systems on the Open IONet:

- a. Penetration testing, such as network scanning, by the project is prohibited. Projects can request the NSO to perform penetration testing. All penetration tests will be conducted by ISAT Personnel.
- b. Network scanning of a project's local sub-networks by the project is permitted if prior NSO authorization is obtained.
- c. Network scanning of a project's local sub-networks by the project is permitted if prior NSO authorization is obtained.
- d. Projects may have IDSs on their own sub-networks. Prior NSO authorization must be obtained. All components of the IDS must be within the project's local Open IONet sub-networks.
- e. Projects may have IDSs on their own sub-networks. Prior NSO authorization must be obtained. All components of the IDS must be within the project's local Open IONet sub-networks.
- f. VPN, or encrypted tunnels, within the Open IONet may be approved. They must be authorized by the NSO and are authorized on a case-by-case basis.

- g. Firewalls are permitted. Firewalls must meet the additional requirements for boundary systems given in Security of Information Technology, NPG 2810.1.

7.3.5.3.3 Hardware Restrictions

The security environment of the IONet hardware is enhanced by physical security and limited access.

7.3.5.3.4 Hardware Restrictions on Closed Segment

The following hardware restrictions apply to IT resources connected to the Closed IONet:

- a. Access from modem and other networks are prohibited.
- b. IONet personnel must control ALL muxes, switches, hubs, firewalls, and routers connecting projects or centers to the Closed Segment.
- c. Physical access to all equipment (including workstations or computers) connected to Closed IONet must be restricted, in accordance with, IONet Access Protection Policy and Requirements, 290-004, Section 5.3.
- d. Dual-homed systems including firewalls are prohibited. A dual homed IT resource has two or more network interfaces, connecting it to two or more different networks.
- e. Projects may have IDSs on their own sub-networks. All components of the IDS must be within the project's local Closed IONet sub-networks. Prior NSO authorization must be obtained.

7.3.5.3.5 Hardware Restrictions on Open Segment

The following hardware restrictions apply to equipment connected to the Open IONet:

- a. Modem and Internet connections are permitted. However, only particular modems are allowed and they are approved on a case-by-case basis by the NSO.
- b. Physical access to all IONet equipment must be restricted, as specified in IONet Access Protection Policy and Requirements, 290-004, Section 5.3.
- c. Dual-homed systems including firewalls will be configured to meet the boundary systems requirements given in Security of Information Technology, NPG 2810.1.
- d. Remote services such as finger and portmapper must be blocked from the Internet.
- e. Projects may have IDSs on their own sub-networks. Prior NSO authorization must be obtained. All components of the IDS must be within the project's local Open IONet sub-networks.

- f. VPNs, or encrypted tunnels, within the Open IONet may be approved. They must be authorized by the NSO on a case-by-case basis.

7.3.5.3.6 Communications Controls

The configuration of all IONet supplied components is accomplished within the physical confines of the IONet facilities and is thus afforded the protection of the GSFC and building security.

7.3.5.3.7 Communication Restrictions on Closed Segment

The following restrictions apply to equipment connected to the Closed IONet:

- a. Traffic between the Closed IONet and the Open IONet must go through the Nascom Secure Gateway.
- b. Only a Closed IONet project/user may request connections (i.e. firewall rules) to the Open IONet through the Nascom Secure Gateway.
- c. Only systems on the Closed IONet may initiate communication to systems on the Open IONet. Exceptions require NSO approval.
- d. Development systems are not permitted on the Closed IONet.
- e. Disable unused Transmission Control Protocol/Internet Protocol (TCP/IP) services on servers and host systems attached to the Closed IONet.
- f. VPN or tunneled traffic through the Nascom Secure Gateway is prohibited. Therefore, VPN traffic between the Open and Closed networks is prohibited.
- g. Encrypted data traffic is permitted within the Closed IONet sub-networks only. However, no troubleshooting will be provided. Advise IPNOC when using encrypted data transmissions.

7.3.5.3.8 Communication Restrictions on Open Segment

The following restrictions apply to equipment connected to the Open IONet:

- a. Traffic to and from the Closed IONet must go through the Nascom Secure Gateway.
- b. Restrict router access to the Open IONet to known/trusted IP addresses.
- c. Disable unused TCP/IP services on servers and host systems attached to the Open IONet.
- d. VPN traffic through the Nascom Secure Gateway is prohibited. Therefore, VPN traffic between the Open and Closed networks is prohibited.
- e. Encrypted data traffic is permitted. However, no troubleshooting will be provided. Advise IPNOC when using encrypted data transmissions.

7.3.5.3.9 Individual Accountability

Access to and use of the IONet must comply with IONet Access Protection Policy and Requirements, Document Number 290-004, which requires individual accountability.

7.3.6 Contingency Plan

The ISAT first level of contingency planning for the IONet is accomplished by providing redundant paths and equipment for all users. A Disaster Recovery Plan contains detailed procedures and instructions in the event of a minor, major, or catastrophic disaster to the IONet.

The basic IONet contingency plan contains the standard operating procedures. A management supplement to the plan provides additional details, such as individual actions, a contact list, and localized procedures.

7.3.6.1 Internet Protocol Operations Network Information Technology System Hardware or Software Protection Loss

Procedures to maintain adequate protection for the IONet network in the event of failure of hardware and software security are described in the Internet Protocol Operational Network (IONet) Disaster Recovery Plan, 290-013.

7.3.6.2 Destruction of System Files, Programs, or Procedural Documentation

Operational provisions are made to make and maintain duplicate copies of all essential software, program documentation, and procedures to protect against their accidental loss. These provisions are to be evaluated at least once yearly to ensure their adequacy and effectiveness.

7.3.6.3 Review and Testing

Contingency plans are reviewed and tested periodically (at least every 3 years or upon significant change). Portions of the plan may be tested throughout the year (rather than testing the entire plan at one time) to minimize disruptions to operations.

7.3.7 Audit and Variance Detection

There are two network monitor workstations running Hewlett Packard (HP) OpenView software in the GSFC Operations Control area that provide 24-hour monitoring for the IONet. The network is monitored every five minutes by using SNMP and ping. If there is a change or a connectivity problem, software detects the change and alerts the operator using an audible alarm and a popup window that describes the equipment in question. The GSFC Communications Manager (COMMGR) is notified immediately. Trouble calls can be placed to the COMMGR at 301-286-6141.

Operating logs which detail system activity are provided automatically by the IONet monitoring system. Operator logs are reviewed daily by the System Operators to ensure that no actions have occurred that affected the security of the system. For each

transaction entered, the information contained on the log is sufficient to meet operating, security analysis, review, and reporting purposes.

7.3.8 Hardware/Application Software Maintenance Controls

The ISAT CCB exercises Configuration Management (CM) of the IONet. Changes are accomplished by a Configuration Change Request (CCR). Changes to the physical structure (facility) are accomplished through Work Orders (WO).

Forms, procedures, reviews, audits and other factors in the CM process are described in the ISAT Configuration Management Plan, 290-001.

7.3.9 Documentation

The following documentation is required for new connections to the IONet:

- a. Security Plan.
- b. Risk Analysis.
- c. Completed checklist to IONet Security Team.
- d. Authorization to Process signed by the Government DAA or Project manager.
- e. Logon banner on all NASA-owned or NASA-funded IT systems.
- f. Statement of Responsibility signed by users.
- g. In addition NASA Headquarters or the Federal Government requires the following:
 1. Contingency/Disaster Recovery Plan.
 2. Annual Computer Security Awareness Training.

7.3.10 Security Awareness and Training Measures

All users and operations personnel for the IONet must be provided Computer Security Awareness Training (CSAT).

The security awareness program must provide:

- a. Security orientation for all new employees.
- b. Security indoctrination for employees requiring access to IONet information.
- c. Periodic (at least annually) security reorientation and refresher briefings or bulletins are required.

7.3.11 Technical Controls

7.3.11.1 User Identification and Authentication

User identification and authentication is performed through use of login ID and password.

- a. Password requirements:
 - 1. Eight (8) characters or longer.
 - 2. Composition includes 3 of the following 4 categories: upper case letters, lower case letters, special characters, and numbers.
 - 3. Changed every 90 days for normal users, 30 days for root and privileged users.
 - 4. Accounts are disabled if password not changed within 30 working days of change period.
- b. Revalidate users annually.
- c. Workstations and computers must be logged off or paused during periods of inactivity unless manned 24 hours a day.

7.3.11.2 Process for Obtaining Security Authorization to Connect to the Internet Protocol Operational Network

The steps a project must take to obtain authorization to connect to the IONet are as follows:

- a. Security Team contacts project representative and sends a soft copy of the Compliance checklist.
- b. The project personnel complete the checklist for their system requesting an IONet interface.
- c. Project personnel contacts the Security Team for forwarding instructions for the checklist(s).
- d. The Security Team evaluates the completed checklist and conducts a physical audit, if necessary.
- e. The Security Team prepares and delivers a security report to the NSO, who recommends approval or denial of connection request.
- f. NSO sends connection approval/rejection to the project manager.

Appendix A. Abbreviations and Acronyms

ADM	Administrative
CCB	Configuration Control Board
CCR	Configuration Change Request
CCSM	Center Computer Security Manager
CEN	Central
CIO	Chief Information Officer
CM	Configuration Management
COMMGR	Communications Manager
CSAT	Computer Security Awareness Training
CSO	Computer Security Official
CSOC	Consolidated Space Operations Contract
DAA	Designated Approving Authority
DCCSM	Deputy Center Computer Security Manager
DCN	Document Control Number
DRD	Data Requirements Directive
ENMC	Enterprise Network Management SystemsCenter
FDDI	fiber distribution data interface
FSO	Facility Security Officer
FTP	File Transfer Protocol
GSFC	Goddard Space Flight Center
GSS	General Support System
HP	Hewlett-Packard
ID	Identification
ID/IR	Intrusion Detection/Incident Response
IDS	Intrusion Detection Systems
IONet	Internet Protocol Operational Network
IP	Internet Protocol

IPSO	Information Processing Service Organization
ISAT	Information Services and Advanced Technology
ISP	Internet Service Provider
ISSO	Information Systems Security Official
IT	Information Technology
ITS	Information Technology System
ITSWG	Information Technology Security Working Group
LAN	Local Area Network
MOA	Memoranda of Agreement
MPG	Marshall Procedures and Guidelines
MSN	Mission
NASA	National Aeronautics and Space Administration
Nascom	NASA Communications
NHB	NASA Handbook
NIS	Network Information Service
NISN	NASA Integrated Services Network
NM	Network Manager
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines
NRP	NASA Resource Protection
NSO	Network Security Officer
NT	New Technology
OCSM	Organization Computer Security Manager
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCITS	Principal Center for Information Technology Security
PIP	Premium Internet Protocol
PrISMS	Program Information Systems Mission Services
SCR	Software Change Request
SER	Scientific, Engineering, & Research
SH	Safety and Health

SIP	Standard Internet Protocol
SM	Security Manager
SMS	System Management Services
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
ST&E	Security, Test, and Evaluation
STD	Standard
TCP/IP	Transmission Control Protocol/Internet Protocol
ViTS	Video Teleconferencing System
VoTS	Voice Teleconferencing System
VPN	Virtual Private Network
WAN	Wide Area Network
WO	Work Order
WWW	World Wide Web

NASA Integrated Services Network (NISN) Security Management Plan

Revision 1